UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

THE PREMISES LOCATED AT 6942 COLONIAL WOODS DRIVE, APT. 70, SAINT LOUIS, MO, 63129, LOCATED IN THE EASTERN DISTRICT OF MISSOURI.

Case No. 4:23-MJ-6266 PLC

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 U.S.C. § 2251(a) or (c) and (e) (the sexual exploitation of children and attempts and conspiracies to do so) and 18 U.S.C. § 2252A (distribution, receipt, and possession of child pornography)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Nicholas W Zotos

Applicant's signature

Nicholas Zotos, Special Agent

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date: 09/22/2023

Patricia L. Cohen

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: Nathan Chapman

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT **6942 COLONIAL WOODS DRIVE, APT. 70, SAINT LOUIS, MO, 63129**, LOCATED IN THE EASTERN DISTRICT OF MISSOURI.	No. 4:23-MJ-6266 PLC SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since November 2017. I am currently assigned to the HSI office in Saint Louis, Missouri and am affiliated with the Missouri Internet Crimes Against Children Task Force. I investigate federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I completed training on these and related topics through the Federal Law Enforcement Training Center (FLETC), the National Criminal Justice Training Center, the National Law Enforcement Training on Child Exploitation, and through various in-service trainings offered through my agency and external partners. That training includes the requirement to observe, review, and classify numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in several forms of electronic media. I am a graduate of the Treasury Computer Forensic Training Program's Basic Computer Evidence Recovery Training and Basic Mobile Device Forensics courses. I hold an A+ certification from the Computing Technology Industry

Association. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including the entire property located at 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129 (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations or attempted violations of 18 U.S.C. §§ 2251 and 2252A, which items are more specifically described in Attachment B of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations or attempted violations of 18 U.S.C. § 2251(a) or (c) and (e) (the sexual exploitation of children and attempts and

conspiracies to do so) and 18 U.S.C. § 2252A (distribution, receipt, and possession of child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2251(a) and (e) prohibit any person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in, or transporting any minor in or affecting interstate or foreign commerce with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed; or if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer; or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed; or attempting or conspiring to do so.

b. 18 U.S.C. § 2251(c) and (e) prohibit any person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in, any sexually explicit conduct outside of the United States, its territories or possessions, for the purpose of producing any visual depiction of such conduct, if the person intends such visual depiction to be transported to the United States, its territories or possession, by any means, including by using any means or facility of

interstate or foreign commerce or mail; or if the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail; or attempting or conspiring to do so.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates

what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer software," as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

m. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

s. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

t. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

u. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

v. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

w. "Webcam," as used herein, refers to a video camera that attaches to a computer or that is built into a laptop or desktop screen. It is widely used for video calling as well as to continuously monitor an activity and send it to a Web server for public or private viewing. Webcams generally have a microphone built into the unit or use the computer's microphone for audio.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. The investigation, described more fully below, involves individuals who have engaged in the sexual exploitation of children through an internet-based, videoconferencing and chat application ("Skype"). Based on the investigation, there is probable cause to believe that an individual who is residing at the SUBJECT PREMISES has, among other things, used a particular account on Skype ("xflinkx") to engage or attempt to engage in the sexual exploitation of minors in violation of the above federal criminal statutes, and that evidence of that conduct will be found at the SUBJECT PREMISES.

Background on Skype

7. Based on my training, experience, and review of publicly available information, I know that Skype is a software product that allows users to conduct live video chats and voice calls with other users over the internet. Skype users can also send instant messages, exchange files and images, send video messages, and conduct multi-person conference calls. Skype is available for

use on personal computers as well as smartphones, tablets, and other electronic devices. Users can sign up for an account and access Skype directly through Skype's website; alternatively, users can download the application, which allows them to access Skype from computers, tablets, cellular phones, certain televisions, and other electronic devices.

8. To access Skype, subscribers must create an account. Skype assigns a subscriber a unique name or ID, and a subscriber can then add a display name to their account. The user can change the display name at any time. The unique name or ID, by contrast, cannot be changed by the user.

9. Skype records some IP addresses associated with user activity, including the original IP address used for the creation of the account and the IP addresses captured at the time the user logs in to Skype. Skype may preserve chat communications and media content, including videos and images exchanged in chat conversations. Whether content is stored and retained, however, is a user-driven setting—that is, the user can determine whether the content will be retained. Skype does not store or retain the content of live video transmissions.

Background on Online Child Sex Trafficking and Exploitation via Webcam and the Internet

10. HSI is investigating individuals who provide access to pre-produced child sexual abuse material and live-streaming online webcam shows involving the sexual abuse of children to paying customers worldwide. This growing transnational child-sexual-abuse industry includes child sex traffickers in, among other places, the Philippines, who collect viewership fees from vetted customers scattered throughout the world. Paying customers often request that these child sex traffickers provide pre-recorded depictions of minors engaging in sexually explicit conduct or sexually abuse minors in real time during private webcam interactions on a variety of streaming video services and applications, including Skype.

11. Based on my training, experience, and information conveyed to me by other law enforcement agents involved in the investigation of live-streaming depictions of child sexual abuse, I know that it is common for such traffickers in the Philippines and elsewhere to be communicating with a large number of individuals who are paying for access to such material. I also know that it is common for the paying customers to be communicating with other traffickers—and sometimes many other traffickers—who are selling access to similar material over the internet. These individuals often use a variety of money service businesses to pay the traffickers or associates of the traffickers for access to this material, including Western Union, WorldRemit, MoneyGram, PayPal, Xoom, and Remitly. In many instances, customers and traffickers must change payment platforms or create multiple accounts on the same platform using slightly changed identifying information to outpace the efforts of payment platforms in detecting suspicious activity and suspending or disabling accounts deemed as engaging in suspicious transactions.

12. I also know that the purchasing individuals often find ways to capture the live-streamed child sexual abuse and exploitation, either by recording the live shows onto their computers or taking still photographs (including "screen captures" or "screen shots") of the abuse, which can also be stored on the individual's computer or an electronic storage device. Such individuals often also save any pre-produced child sexual abuse material the traffickers provide to their computer or an electronic device for later viewing or re-distribution.

13. In February of 2023, your affiant received reports from HSI Portland. Based on your affiant's review of the reports, I learned the following:

a. HSI has identified an individual (hereinafter referred to as the "TRAFFICKER") operating a child-sex-trafficking network from the Philippines. Based on undercover activity and other investigation, HSI is aware that the TRAFFICKER did,

in fact, have access to minors to sexually abuse on camera and has offered to provide access, through the TRAFFICKER's account on Skype, to visual depictions of one or more minors engaging in sexually explicit conduct in exchange for money.

b. On March 25, 2022, the United States District Court of Maine issued federal search warrant (2:22-MJ-50-JAW) for records pertaining to the Skype account used by the TRAFFICKER. In response, Microsoft provided HSI with information associated with that account on May 13, 2022, and provided additional records on June 8, 2022. The information provided by Microsoft revealed incriminating chat content between the TRAFFICKER and Skype account "xflinkx." Subsequent summons to Microsoft revealed Skype account "xflinkx" lists otaku_sanel@sbcglobal.net as the current email address associated with that account. Your affiant personally reviewed the portion of the search warrant response which included account "xflinkx" and personally reviewed the summons response related to that account.

14. Between March 3, 2023, and September 18, 2023, your affiant obtained and served 25 Department of Homeland Security (DHS) summons requesting information from various electronic service providers, money services businesses, and other entities to ascertain information pertaining to the Skype username "xflinkx," the otaku_sanel@sbcglotal.net email address, and their user. Based on the responses to DHS summons, your affiant reviewed records from Yahoo, Inc., PayPal Inc., Microsoft, Xoom, Moneygram, WorldRemit Corp, Google, T-Mobile, and Charter Communications.

15. Your affiant reviewed the available IP connection history for the "xflinkx" Skype account provided by Microsoft and found an IP address capture associated with the account's "Last Modified Date and Time" on August 31, 2019. I then queried that IP address with Charter

Communications who provided records showing the subscriber using that IP address at the time as Brana Smajlovic with both billing and service address listed as SUBJECT PREMISES, and with phone number as 314-255-6957.

16. Based on your affiant's review of records from T-Mobile, phone number 314-255-6957 is registered to Sanel SMAJLOVIC with service address as SUBJECT PREMISES.

17. Based on your affiant's review of records from Yahoo, Inc, I learned a user created email address otaku_sanel@sbcglobal.net on October 5, 2006, and provided initials "SS" in the field asking for first and last name.

18. Your affiant reviewed records from PayPal Inc, for all accounts associated with the otaku_sanel@sbcglobal.net email address and learned there are a total of 10 active or inactive accounts which used that email address. Seven of those accounts are in the name of Sanel SMAJLOVIC who is 33 years old and resides at SUBJECT PREMISES. Two other accounts are in the name of Halid Smajlovic, who is 65 years old, and use the same SUBJECT PREMISES on the account. The final account, which is inactive, uses the same SUBJECT PREMISES and is in the name of Brana Smajlovic, who is 58 years old. The Halid or Brana Smajlovic accounts do not have transaction history within the last five years. Seven out of the ten accounts, including the two accounts in the name Halid Smajlovic, list phone number 314-255-6957 subscribed to Sanel SMAJLOVIC. Two more accounts in the name of Sanel SMAJLOVIC do not list phone number at all.

19. On April 12, 2023, your affiant applied for and was granted a search warrant (4:23-MJ-8078 SRW) for records pertaining to Skype account "xflinkx," held by Microsoft Corporation. Microsoft responded to that warrant on July 10, 2023, and your affiant has/continues to review the records. The response from Microsoft included over 58,000 lines of chat between "xflinkx" and

722 unique usernames, between April 20, 2017, and September 14, 2022. Your affiant's review of that material is ongoing but revealed numerous examples of the user of "xflinkx" soliciting or negotiating for, and in many instances seemingly completing, online live video sex shows involving minor females in the Philippines as young as one year old. The chat logs were explicit enough to make clear "xflinkx" was knowingly paying for and directing sex acts be performed on minors in a live international broadcast. In some instances, the traffickers would send photographs as a sample or advertisement of the minor girls available for "xflinkx" to purchase a show with. Some of these sample images themselves displayed minors engaged in sexually explicit conduct. A more detailed sample of these transactions is contained in paragraph 32 below.

20. Contained within the Microsoft warrant return are several instances where the user of "xflinkx" self-identified himself as Sanel SMAJLOVIC in conjunction with providing payment confirmation details to the traffickers in the Philippines. To be sure, your affiant was able to cross-reference the date, time, payment amount, and recipient information discussed in the sex trafficking chats with financial transactions from Money Service Business accounts directly linked to Sanel SMAJLOVIC and listing his home address as SUBJECT PREMISES.

21. In other conversations, the user of "xflinkx" identified himself as Sanel in a more social context and refenced employment for the Federal Reserve Bank. Your affiant consulted with the Federal Reserve Board Office of Inspector General (OIG) and confirmed Sanel SMAJLOVIC is employed by the Federal Reserve Bank of Saint Louis and has been so employed since October 30, 2017. Your affiant viewed a public LinkedIn profile for "Sanel S.", which lists his employment as a Senior Software Engineer for the Federal Reserve Bank of Saint Louis. The OIG also provided your affiant with information from Sanel SMAJLOVIC's personnel file which listed a home address of record, as SUBJECT PREMISES.

Financial Transactions Involving SUBJECT PREMISES

22. Based on your affiant's review of records from Xoom, SUBJECT PREMISES is the listed address for Sanel SMAJLOVIC's Xoom Account 10821485. Xoom is a PayPal Inc service that operates as a money service business. That account made 36 payments to the Philippines from May 2018 to September 2019, including at least 12 payments that were cross-referenced to actual sex trafficking shows from the chat log.

23. Based on your affiant's review of records from MoneyGram SUBJECT PREMISES is also the sender's address for at least 47 MoneyGram payments from Sanel SMAJLOVIC to various recipients in the Philippines between January 2017 to February 2018.

24. Based on your affiant's review of records from Western Union, SUBJECT PREMISES is also the sender's address for at least five Western Union payments from Sanel SMAJLOVIC to various recipients in the Philippines between December 6, 2013, and March 1, 2018.

25. Based on your affiant's review of records from WorldRemit, SUBJECT PREMISES is also the sender's address for at least one attempted WorldRemit payment from Sanel SMAJLOVIC to a recipient in the Philippines on July 11, 2017.

Identification of the SUBJECT PREMISES

26. The Missouri Information Analysis Center queried public records databases that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information. These public records indicated that SMAJLOVIC's current address is SUBJECT PREMISES.

27. Your affiant queried the Missouri Department of Motor Vehicles records on or about September 19, 2023, revealed that an individual named Sanel SMAJLOVIC with a date of

birth of xx/xx/1989, resides at the SUBJECT PREMISES. In addition, a 2001 Toyota bearing Missouri registration TA1X0E is registered to Halid and Sanel Smajlovic at SUBJECT PREMISES. This registration was just recently renewed on August 18, 2023.

28. On or about September 19, 2023, your affiant spoke to a representative of the U.S. Postal Service who stated that an individual or individuals with the family name Smajlovic are currently receiving mail at the SUBJECT PREMISES.

29. On September 21, 2023, your affiant spoke to a representative with Ameren electric utility who reported Halid Smajlovic is the customer of record for SUBJECT PREMISES and has been since 2011.

30. Your affiant performed surveillance of the SUBJECT PREMISES on or about September 19, 2023, and observed the 2021 Toyota registered to Halid and Sanel Smajlovic is parked on a surface parking lot adjacent to SUBJECT PREMISES.

31. Your affiant's review of Sanel SMAJLOVIC's international travel records revealed he departed the United States on September 1, 2023, from Lambert International Airport destined to Romania via Frankfurt, Germany and is scheduled to return to the United States via Lambert International Airport on Sunday September 24, 2023. Your affiant along with other customs officers at Lambert International Airport encountered SMAJLOVIC during a routine outbound currency inspection as he left the United States. SMAJLOVIC reported the purpose of his travel was to visit friends.

32. According to ECPAT, a global network of civil society organizations that works to end the sexual exploitation of children, Romania is a "well established destination country for child sex tourists." According to the 2018 European Commission's Report on Trafficking in Human Beings in the European Union (EU), the top member states of citizenship of registered

victims in the 2015-2016 period were Romania, Hungary, the Netherlands, Poland and Bulgaria. The US State Department reported in their 2023 Trafficking in Persons Report that, "Romania remains a primary source country for sex trafficking and labor trafficking victims in Europe." The report further classified Romania as a country "whose governments do not fully meet the [Trafficking Victims Protection Act of 2000] TVPA's minimum standards but are making significant efforts to bring themselves into compliance with those standards."

33. On September 13, 2023, a Grand Jury for the Eastern District of Missouri returned a sealed indictment charging SMAJLOVIC with four counts of attempted production of child pornography. (4:23-CR-00490-SRC-RHH). These four counts relate to the investigation outlined above. A sampling of SMAJLOVIC's chat records for each count is as follows:

a. For Count I, the SMAJLOVIC corresponded with a user (hereinafter, "TRAFFICKER 2") over Skype on February 9, 2019. SMAJLOVIC is told that TRAFFICKER 2 is offering a five-year-old child and 10-year-old child, and a price is eventually negotiated. During the live stream, the SMAJLOVIC makes the following requests/statements to TRAFFICKER 2; "yes do fingering," "put finger in straight I can't see like that," "I want see it go inside hehe," and "show me both girls open pussy." The live stream ends, and TRAFFICKER 2 confirms that he/she has received the SMAJLOVIC's payment.

b. For Count II, the SMAJLOVIC corresponded with TRAFFICKER 2 on August 17, 2019. SMAJLOVIC is told that TRAFFICKER 2 is offering an 11-year-old child, and a price is eventually negotiated. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 2; "ye shes nice cute girl but I like 3-5 more ehe(sic). Even 1-3 sometimes haha," "how deep u can put finger her?", "finger all

inside?", "ok hun this time I do for that girl but try find me younger hehe. Or some girl before but more deep? Hehe." When TRAFFICKER 2 tells SMAJLOVIC, "its deep now she getting hurt now," SMAJLOVIC responds, "more deep hun." The live stream ends, and TRAFFICKER 2 confirms that he/she received SMAJLOVIC's payment.

c. For Count III, SMAJLOVIC corresponded with a different user (hereinafter, "TRAFFICKER 3") on October 6, 2018. SMAJLOVIC is told that TRAFFICKER 3 is offering a one-year-old child. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 3; "and lol what u can do with the 1? Nothing? I think too young for me but can I see? Hehe," "can you open lips more? Hehe," "finger her? Or no?", and "nice hehe." SMAJLOVIC eventually provides TRAFFICKER 3 with payment on October 16, 2018.

d. For Count IV, SMAJLOVIC corresponded with TRAFFICKER 3 on June 23, 2018. SMAJLOVIC is told that TRAFFICKER 3 is offering a six-year-old child and ten-year-old child, and a price is negotiated. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 3; "can u wake the 6?", "I like her more," "ye…wake her for show? Or let her sleep u can still show her hehe," and "tell the 10 to put finger in the 6yo pussy hehe." The live stream ends, and TRAFFICKER 3 confirms that he/she has received the SMAJLOVIC's payment.

34. Your affiant's review of the chat logs pertaining to Skype account "xflinkx" revealed this type of activity occurred until at least August 31, 2019. Your affiant's diligent search of available law enforcement databases revealed no intervening law enforcement action that would have stopped SMAJLOVIC from continuing this conduct. In my experience with similar investigations and in consultation with other law enforcement investigating child sex traffickers in

the Philippines, it is common for traffickers and customers to change out account usage on various chat applications, including Skype. In fact, in the chat logs from Microsoft I found examples where the user of "xflinkx" references knowing traffickers from their other username or ID or from other chat rooms or platforms.

35. Accordingly, based on my training and experience and the information articulated herein, I submit that there is probable cause to believe that Sanel SMAJLOVIC, residing at the SUBJECT PREMISES, used the internet to knowingly and intentionally attempt to produce child pornography.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

36. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and

tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child

pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN OR WHO PRODUCE, RECEIVE, AND/OR POSSESS CHILD PORNOGRAPHY

37. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a

computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the individual's home, the SUBJECT PREMISES, as set forth in

Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

38. Based on all the information contained herein, I believe that an individual residing at the SUBJECT PREMISES likely displays characteristics common to individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography. In particular, the target of the investigation used the Skype Account "xflinkx" to specifically direct sexual acts that cause pain to children and openly professed preference or attraction to children below 10 years of age, and in some instances one to three years of age.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

39. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

41. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further,

computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent

or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable

to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

43. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which

create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

44. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

45. This warrant permits law enforcement to compel Sanel SMAJLOVIC to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through their fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through their face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of their face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices

produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with their irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers their irises by holding the device in front of their face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access

the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Sanel SMAJLOVIC to the fingerprint scanner of the devices found at the PREMISES; (2) hold the devices found at the PREMISES in front of the face of Sanel SMAJLOVIC and activate the facial recognition feature; and/or (3) hold the devices found at the PREMISES in front of the face of Sanel SMAJLOVIC and activate the iris recognition feature, for the purpose of attempting to

unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Sanel SMAJLOVIC state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel Sanel SMAJLOVIC to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

46. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

47. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

48. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their

premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

NICHOLAS ZOTOS
Special Agent
Homeland Security Investigations

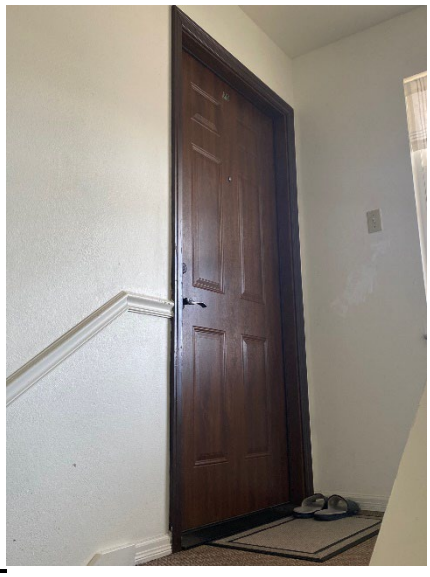
Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 22nd day of September 2023.

Patricia L. Cohen
HONORABLE PATRICIA L. COHEN
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129 (the SUBJECT PREMISES), a second story walk up apartment in a multi-unit apartment complex, the exterior building has brick siding and "6942" labeled on a cream or tan door, Apt 70 is on the second floor behind a brown door with "70" labeled on the top, and any person located at the SUBJECT PREMISES.



The person of Sanel SMAJLOVIC (DOB: xx/xx/1989), provided that this person is located at the SUBJECT PREMISES and/or within the Eastern District of Missouri at the time of the search.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2251:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

    a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129, including utility and telephone bills, mail envelopes, or addressed correspondence;

    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

    d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Sanel SMAJLOVIC to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found at the SUBJECT PREMISES, and

b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to require that Sanel SMAJLOVIC state or otherwise provide the password or any other means that may be used to unlock or access the devices,including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.